



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/072,147	02/07/2002	Tomi Hakkarainen	4208-4027	1454
27123	7590	06/26/2006	EXAMINER	
MORGAN & FINNEGAN, L.L.P. 3 WORLD FINANCIAL CENTER NEW YORK, NY 10281-2101				DINH, MINH
		ART UNIT		PAPER NUMBER
		2132		

DATE MAILED: 06/26/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	10/072,147	HAKKARAINEN ET AL.
	Examiner	Art Unit
	Minh Dinh	2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 10 April 2006.
- 2a) This action is FINAL. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-36 and 39-41 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) Claim(s) _____ is/are allowed.
- 6) Claim(s) 1-36 and 39-41 is/are rejected.
- 7) Claim(s) _____ is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on 07 February 2002 is/are: a) accepted or b) objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)	4) <input type="checkbox"/> Interview Summary (PTO-413)
2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)	Paper No(s)/Mail Date. _____.
3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.	5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)
	6) <input type="checkbox"/> Other: _____.

DETAILED ACTION

Response to Amendment

1. This action is in response to the amendment filed 04/10/2006. Claims 1, 21, 25 and 39 have been amended; claims 37-38 have been cancelled; claims 40-41 have been added.

Response to Arguments

2. Applicant's arguments with respect to claim 1 have been considered but are not persuasive. Applicant's amendments have necessitated a new search and new grounds of rejection.

3. Applicant's arguments filed 04/10/2006 with respect to the rejections of claims 33-34 have been fully considered but they are not persuasive. Claim 33 is dependent upon claim 25, which recites the limitation: "receiving the service over a unidirectional channel". Claim 33 itself recites the limitation: "determining whether the service has been dropped; **if** the service has been dropped, determining whether either the first decryption information or the second decryption information is valid decryption information; **if** one of the first decryption information or the second decryption information is valid decryption information, **decrypting the service with the valid decryption information**". Claim 33 was rejected

in the previous Office Action because the claim limitation is contradictory, i.e., since it is determined that the service has been dropped, the service is not available and thus there is no service to decrypt. Applicant argues that claim 33 is “open-ended” through its use of the term “comprising” and thus, **does not preclude the client from receiving the encrypted service again prior to the performance of the remaining steps of claim 33** (Remark, page 10). Based on the language of claim 33, the step of “decrypting the service with the valid decryption information” only happens under two conditions. Now, with Applicant’s argument, one more condition must be met (i.e., the client receives the encrypted service again) in order for the step of decrypting the service to happen. One of ordinary skill in the art would not be expected to figure out the scenario applying to claim 33 that the client receives the encrypted service again after the service has been dropped, especially when Applicant’s reasoning and illustrating example provided in the remark were not disclosed in the originally filed specification. Thus, the disclosure fails to enable one skilled in the art to make and use the claimed invention.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to

enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

5. Claims 2-3 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. Claim 2 recites the limitation "wherein the first decryption information corresponds to a seed of a macro period". Claim 2 is dependent upon claim 1, which recites the amended feature "wherein the first decryption information decrypts the service". The originally filed specification does not disclose that the seed of a macro period decrypts the service. The specification only discloses that that the seed of a macro period decrypts the key of the first micro period of the macro period (page 6, last paragraph; figure 2). As a result of the amended claim 1, the feature of claim 2 is considered new matter. Claims that are not specifically addressed are rejected by virtue of their dependency.

6. Claims 33-34 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as

to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. Claim 33 is dependent upon claim 25, which recites the limitation: "receiving the service over a unidirectional channel". Claim 33 itself recites the limitation: "determining whether the service has been dropped; if the service has been dropped, determining whether either the first decryption information or the second decryption information is valid decryption information; if one of the first decryption information or the second decryption information is valid decryption information, decrypting the service with the valid decryption information". The condition "the service has been dropped" is interpreted as "the service is not available". If the service is not available because the connection has been dropped, then there is no service to decrypt. If the connection has not been dropped and the service is not available because there is no valid decryption key, then the question is why a valid key can still be found to decrypt the service. The claim is contradictory, and as a result, the disclosure fails to enable one skilled in the art to make and use the claimed invention. For examination purposes, the claim limitation is interpreted as "determining whether either the first decryption information or the second decryption information is valid decryption information; if one of the first decryption information or the second decryption information is

valid decryption information, decrypting the service with the valid decryption information".

Claim Rejections - 35 USC § 102

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

1. Claims 1-3, 6-9, 12-13, 16-19, 21, 25-26, 28-29, 35-36 and 39-41 are rejected under 35 U.S.C. 102(e) as being anticipated by Raith (6,510,515).

Raith discloses a method for controlling access to encrypted broadcast services such as stock quotes and sports news (Abstract).

Regarding claims 1-3, 6-7, 16-17, 21, 25-26, 36 and 39-40, Raith discloses a method for a requester to order a service and for a service provider to provide, in response to the request, the ordered service in an encrypted form and keys necessary to decrypt the encrypted broadcast service, comprising: receiving a request for a service from a requestor over

a bi-directional channel; authenticating the requestor (col. 12, line 17-67); transmitting first decryption information, a service decryption key, to the requestor over the bi-directional channel wherein the service decryption key decrypts; transmitting the service, encrypted with encryption information corresponding to the first decryption information, over a unidirectional channel (col. 11, lines 39-50; col. 11, lines 16-26; col. 12, line 17-67); generating second decryption information, a secret value, for use in decrypting the service; transmitting the second decryption information over the unidirectional channel; and transmitting the service, encrypted with encryption information corresponding to the second decryption information, over the unidirectional channel (col. 16; lines 34-51).

Regarding claims 8-9, 12-13, 28-29, Raith further discloses that the bi-directional channel is a GSM network and that authentication is performed using a SIM card number or a PIN number (col. 1, line 60 – col. 2, line 5; col. 3, line 65 – col. 4, line 6; col. 9, lines 61-64).

Regarding claims 18-19, Raith further discloses that the second decryption information itself is used as synchronization information and is encrypted with the first decryption information (col. 16; lines 34-51).

Regarding claim 35, Raith further discloses that the decryption information itself is used as synchronization information and is encrypted with the first decryption information (col. 16; lines 34-51).

Regarding claim 41, Raith further discloses that a key index in order to identify the service decryption key is transmitted to the requestor (col. 9, lines 51-59).

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1, 4-8, 11, 13-27, 29-36 and 39-41 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wasilewski et al. (6,516,412) in view of Roop et al. (5,619,274). Wasilewski discloses a cable TV system providing conditional access to services (e.g., TV programs, CATV channels, movies) encrypted using a control word (CW) that changes periodically (col. 4, line 15 – col. 5, line 12).

Regarding claims 1, 4-7, 11, 14-19, 21-27, 30-32, 35-36 and 39-40, Wasilewski discloses a method for a requester to order a service and for a service provider to provide, in response to the request, the ordered service in an encrypted form and keys necessary to decrypt the encrypted service, comprising: receiving a request for a service from a requestor over a bi-

directional channel (col. 31, lines 25-63; col. 34, lines 1-12); authenticating the requestor using a public key encryption scheme associated with the IP address of the requestor (col. 12, line 46 – col. 13, line 9; col. 34, lines 13-44; col. 42, line 59 – col. 43, line 12); transmitting an authorization message (an entitlement management message - EMM) including a multi-session key to the requestor over the bi-directional channel for use in decrypting the service (col. 4, line 63 – col. 5, line 12; col. 6, lines 25-61; col. 16, line 63 – col. 17, line 13); transmitting the service, encrypted using a control word (CW) that changes periodically, over a unidirectional channel (col. 4, lines 40-45); generating second decryption information corresponding to a micro period which is the control word for use in decrypting the service; transmitting an entitlement control message (ECM) including the control word over the unidirectional channel (col. 6, lines 25-61); and transmitting the service, encrypted with encryption information corresponding to the second decryption information, over the unidirectional channel (col. 6, lines 25-61). Wasilewski does not disclose that an initial control word is included in the authorization message. Roop discloses a conditional access system for providing service encrypted with a program key that changes periodically, the program key being functionally equivalent to Wasilewski's control word. Roop further discloses that when a requestor is authorized, an authorization message including the initial program key to

be used for decryption is transmitted to the requestor (col. 11, lines 25-37; col. 13, lines 1-9). It would have been obvious to one of ordinary skill in the art at the time the invention was made such that the initial control word is included in the authorization message, as taught by Roop. With the initial control word in hand, the requestor's device would be ready to decrypt the service when it was first received. Accordingly, the initial control word would be transmitted to the requestor over the bi-directional channel.

Regarding claim 8, Wasilewski further discloses that the bidirectional channel is one of a wireless network (col. 4, lines 41-43; col. 5, lines 5-9).

Regarding claims 13 and 29, Wasilewski further discloses that the authentication is performed using a user ID and a PIN which meets the limitation of a password (col. 4, lines 45-53).

Regarding claim 20, Wasilewski further discloses retransmitting the second decryption information over a unidirectional channel (col. 4, lines 34-36).

Regarding claim 33, Wasilewski further discloses determining whether either the first or second decryption information is valid decryption information and decrypting the service with valid decryption information (col. 9, lines 12-22, 43-57; col. 38, line 40 – col. 39, line 10).

Regarding claim 34, Wasilewski further discloses that when neither the first decryption information nor the second decryption information is valid

decryption information (e.g., end of month), establishing a connection to the service provider via the bi-directional channel; transmitting authentication information over the bi-directional channel; receiving valid decryption information over the bi-directional channel; and decrypting the service using the valid decryption information (col. 2, lines 21-29; col. 34, lines 1-12).

Regarding claim 41, Wasilewski further discloses that in addition to the initial control word and subsequent control words, a multi-session key is transmitted to the requestor to decrypt the service (col. 6, lines 25-61).

4. Claims 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Wasilewski in view of Roop as applied to claim 8 above, and further in view of Vieweg et al (6,748,082). Wasilewski discloses that the bidirectional channel is one of a wireless network; however, Wasilewski does not disclose that the wireless network is a GSM network. Vieweg discloses using a GSM network (col. 2, line 66 – col. 3, line 2). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method of Wasilewski and Roop to use a GSM network, as taught by Vieweg. It is particularly simple, and, in terms of automatization ability, efficient for transmission to be in the form of a digital mobile radio short message like GSM-SMS (col. 2, lines 45-50).

5. Claims 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over Wasilewski in view of Roop as applied to claim 8 above, and further in view of Gulcu et al (6,925,562). Wasilewski discloses that the bidirectional channel is one of a wireless network; however, Wasilewski does not disclose that the wireless network is a Bluetooth network. Vieweg discloses using a Bluetooth network (col. 2, lines 6-27). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method of Wasilewski and Roop to use a Bluetooth network, as taught by Gulcu. Bluetooth technology would allow users to connect a wide range of devices easily and quickly, without the need for cables, expanding communications capabilities for mobile devices.

6. Claims 12 and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wasilewski in view of Roop as applied to claim 1 above, and further in view of Raith (6,510,515). Wasilewski does not disclose that the authentication is performed using a SIM card number. Raith discloses performing authentication using a SIM card number in a conditional access system (col. 1, line 60 – col. 2, line 10; col. 11, lines 37-60). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method of Wasilewski and Roop such that the

authentication is performed using a SIM card number, as taught by Raith, in order to allow the system to verify the SIM card.

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

U.S. Patent No. 6,738,905 to Kravitz et al.

8. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dinh whose telephone number is 571-272-3802. The examiner can normally be reached on Mon-Fri: 10:00am-6:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

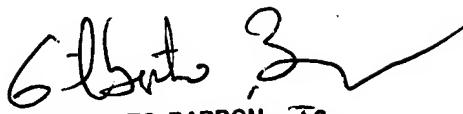
Application/Control Number: 10/072,147
Art Unit: 2132

Page 15

MD

Minh Dinh
Examiner
Art Unit 2132

MD
6/20/06


GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100